(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平８－２３７５９６

(43)公開日　平成８年（１９９６）９月１３日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04N 5/91			H04N 5/91	P	
5/92			5/92	H	
7/167			7/167		

審査請求　未請求　請求項の数３８　ＯＬ　（全１４頁）

(21)出願番号　特願平７－３１８３９８

(22)出願日　平成７年（１９９５）１２月６日

(31)優先権主張番号　１９９４－３３３３６

(32)優先日　１９９４年１２月８日

(33)優先権主張国　韓国（ＫＲ）

(71)出願人　５９０００１６６９
エルジー電子株式会社
大韓民国，ソウル特別市永登浦区汝矣島洞２０

(72)発明者　朴　兌濬
大韓民國，　ソウル市，　種路區，　崇仁洞，　２０－１１８

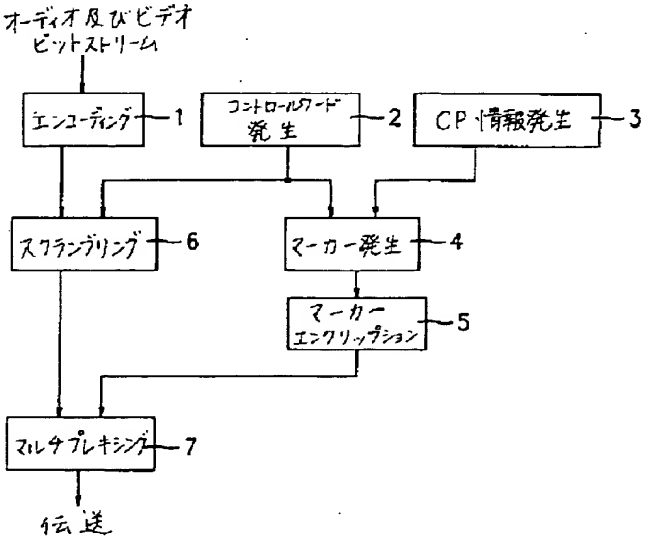
(74)代理人　弁理士　山本　秀策

(54)【発明の名称】ディジタル磁気記録再生システムの複写防止方法及び装置

(57)【要約】

【課題】　プログラム供給者が所望の多様な複写防止機能を実現できるようにしたディジタル磁気記録再生システムの複写防止方法及び装置を提供する。

【解決手段】　本発明によるディジタル磁気記録再生システムの複写防止方法は、オーディオ及びビデオビットストリームをスクランブリングするためのコントロールワードと不法複写防止のためのＣＰ情報により作られたマーカーを暗号化キーを用いてエンクリプションして前記コントロールワードにスクランブリングされたオーディオ及びビデオビットストリームをマルチプレキシングして伝送し、前記伝送されたビットストリームからマーカーを検出し暗号化されたキーを用いてディクリプション及び分析して複写を許容するか否かを決定して検出されたマーカーを更新させビデオテープに記録させ、前記マーカーからコントロールワードを発生してディスクランブリングしてディスプレイできるようにモニターに出力することによりなる。



1

【特許請求の範囲】

【請求項１】　オーディオ及びビデオビットストリームをスクランブリングするためのコントロールワードと不法複写防止のためのコピー防止（ＣＰ）情報とにより作られたマーカーを、暗号化キーを用いてエンクリップションして、前記コントロールワードでスクランブリングされたオーディオ及びビデオビットストリームで、マルチプレキシングして伝送するオーディオ及びビデオ信号伝送工程と、

前記伝送されたビットストリームからマーカーを検出し、暗号化されたキーを用いてディクリップション及び分析して、複写を許容するか否かを決定して、検出されたマーカーを更新させビデオテープに記録させ、前記マーカーからコントロールワードを発生してディスクランブリングして、ディスプレイできるようにモニターに出力するオーディオ及びビデオ信号受信及び記録工程と、

を包含するディジタル磁気記録再生システムの複写防止方法。

【請求項２】　前記マーカーは、前記ビットストリーム内の伝送プライベートデータフィールドに位置する請求項１に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項３】　前記マーカーは、不法複写防止のためのコピー防止（ＣＰ）情報の記録されたコピー防止（ＣＰ）情報領域と、ディスクランブリングのためのコントロールワードが記録されたコントロールワード領域と、

を有する請求項２に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項４】　前記マーカーは、８バイトよりなる請求項３に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項５】　前記コピー防止（ＣＰ）情報領域は、１バイトよりなる請求項４に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項６】　前記コントロールワード領域は、４バイトよりなる請求項４に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項７】　前記コピー防止（ＣＰ）情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマッティングされる請求項３に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項８】　前記世代複写制御フィールドは、プログラムの複写を許す回数を制限するための許容世代フィールドと、

複写されたプログラムの現在の世代を示す現在世代フィールドと、

を有する請求項７に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項９】　前記オーディオ及びビデオ伝送工程は、オーディオ及びビデオビットストリームをエンコーディングするオーディオ及びビデオビットストリームエンコーディング工程と、

スクランブリングのためのコントロールワードを発生するコントロールワード発生工程と、

前記発生されたコントロールワードを用いて前記エンコーディングされたオーディオ及びビデオビットストリームをスクランブリングするスクランブリング工程と、

不法複写防止のためのコピー防止（ＣＰ）情報を発生するコピー防止（ＣＰ）情報発生工程と、

前記発生されたコントロールワードと前記コピー防止（ＣＰ）情報を用いてマーカーを発生し暗号化されたキーを用いてエンクリップションするマーカー発生及びエンクリップション工程と、

前記スクランブリングされたオーディオ及びビデオビットストリームとエンクリップションされたマーカーをマルチプレキシングして伝送するマルチプレキシング及び伝送工程と、

を包含する請求項１に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項１０】　前記オーディオ及びビデオ信号受信工程は、

前記伝送されたビットストリームをディマルチプレキシングしてマーカーを検出し、暗号化されたキーを用いてディクリップションするマーカー検出工程と、

前記検出されたマーカーを分析して複写を許容するか否かを決定しコントロールワードを検出するマーカー分析工程と、

前記検出されたコントロールワードで、前記伝送されたオーディオ及びビデオビットストリームをディスクランブリング及びディコーディングして、音声及び映像信号を出力するオーディオ及びビデオディコーディング工程と、

前記マーカー分析結果複写可能な場合、前記検出されたマーカーを、更新させ暗号化されたキーを用いてエンクリップションして挿入するマーカー挿入工程と、

を包含する請求項１に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項１１】　前記マーカー分析工程は、前記検出されたマーカーから不法複写防止のためのコピー防止（ＣＰ）情報を検出するコピー防止（ＣＰ）情報検出工程と、

前記検出されたコピー防止（ＣＰ）情報内のプログラムの複写を許容する回数を制限するための容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写が可能か否かを判別して処理する複写回数制限工程と、

前記検出されたマーカーより、ディスクランブリングのためのコントロールワードを検出するコントロールワード検出工程と、

を包含する請求項１０に記載のディジタル磁気記録再生

システムの複写防止方法。

【請求項１２】　前記複写回数制限工程は、
前記許容世代フィールドの許容世代と、現在世代フィールドの現在世代とを比較して、前記許容世代が現在世代以下かを判断する工程と、
前記判断結果前記許容世代が現在世代以下なら複写を不可能にする工程と、
前記判断結果前記許容世代が現在世代以下でなければ複写を可能にし、前記マーカー挿入工程に進む工程と、
を包含する請求項１１に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項１３】　前記複写を不可能にする工程は、複写後、再生が不可能になるようにコントロールワードを破壊したり、出力できないようにする請求項１２に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項１４】　前記コントロールワードは、周期的に変化される請求項１０に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項１５】　前記コントロールワードは、０．６秒間隔に変わる請求項１４に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項１６】　前記マーカーは、前記コントロールワードが変わる毎に、前記ビットストリーム内のプライベートデータフィールドに位置する請求項１４に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項１７】　前記マーカ挿入工程は、
前記マーカー分析結果複写可能な場合は前記マーカーを更新させる工程と、
前記更新されたマーカーを暗号化されたキーを用いてエンクリップションする工程と、
前記エンクリップションされたマーカーを次に現れるマーカーと交替して挿入する工程と、
を包含する請求項１６に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項１８】　前記暗号化されたキーは、別途の伝送路を通じて伝送され貯蔵される請求項１に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項１９】　前記暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵される請求項１８に記載のディジタル磁気記録再生システムの複写防止方法。

【請求項２０】　入力されるビットストリームから、マーカーを検出し、更新されたマーカーを、前記ビットストリームに挿入して出力するマーカー検出及び挿入部と、
前記マーカー検出及び挿入部から出力されるエンクリップションされたマーカーを、暗号化されたキーを用いてディクリップションし分析して、ビットストリームをディスクランブリングさせるためのコントロールワードを出力して、ディクリップションされたマーカーを、更新させ暗号化されたキーを用いてエンクリップションさせ出力するマーカー分析及び処理部と、
前記マーカー分析及び処理部から出力されるコントロールワードと、更新されエンクリップションされたマーカーとをバッファリングして、前記更新されエンクリップションされたマーカーを、前記マーカー検出及び挿入部で挿入できるように出力するバッファと、
前記バッファから出力されるコントロールワードを用いて、前記マーカー検出及び挿入部を通じて出力されるビットストリームを、ディスクランブリングするディスクランブラと、
を備えたディジタル磁気記録再生システムの複写防止装置。

【請求項２１】　前記暗号化されたキーは、別途の伝送路を通じて伝送され貯蔵される請求項２０に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項２２】　前記暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵される請求項２１に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項２３】　前記マーカーは、前記ビットストリーム内の伝送プライベートデータフィールドに位置する請求項２０に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項２４】　前記マーカーは、不法複写防止のためのコピー防止（ＣＰ）情報が記録されたコピー防止（ＣＰ）情報領域と、ディスクランブリングのためのコントロールワードの記録されたコントロールワード領域と、を備えた請求項２３に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項２５】　前記マーカーは、８バイトよりなる請求項２４に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項２６】　前記コピー防止（ＣＰ）情報領域は、１バイトよりなる請求項２５に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項２７】　前記コントロールワード領域は、４バイトよりなる請求項２５に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項２８】　前記コピー防止（ＣＰ）情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマッティングされる請求項２４に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項２９】　前記世代複写制御フィールドは、プログラムの複写を許容する回数を制限するための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドと、を備えた請求項２８に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項３０】　前記コントロールワードは、周期的に変わる請求項２０に記載のディジタル磁気記録再生シス

テムの複写防止装置。

【請求項３１】　前記コントロールワードは、０．６秒間隔に変わる請求項３０に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項３２】　前記マーカーは、前記コントロールワードが変わる毎に前記ビットストリーム内のプライベートデータフィールドに位置する請求項３０に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項３３】　前記マーカー検出及び挿入部は、前記更新されたマーカーを次に現れるマーカーと交替して挿入する請求項３２に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項３４】　前記マーカー検出及び挿入部は、
入力されるビットストリームからエンクリプトされたマーカーを検出して、前記マーカー分析及び処理部に出力し、前記ビットストリーム内におけるエンクリプトされたマーカーの位置を知らせるマーカー検出フラグ信号を前記ディスクラブラに出力して、前記ディスクランブラが初期化される基準信号として使われるようにし、ビットストリームを出力するマーカー検出部と、
前記マーカー検出部から出力されるマーカー検出フラグ信号に応じて、前記マーカー検出部から出力されるビットストリームに、前記バッファから出力される更新されエンクリップションされたマーカーを、挿入して、前記ディスクランブラに出力するマーカー挿入部と、
を備えた請求項２０に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項３５】　前記マーカー分析及び処理部は、
前記マーカー検出及び挿入部から出力されるエンクリップションされたマーカーを、暗号化されたキーを用いてディクリップションするマーカー解読部と、
前記マーカー解読部から出力されるマーカー内部のコピー防止（ＣＰ）情報を分析して、複写が許容される場合、前記バッファにコントロールワードを出力しマーカーを更新するための制御信号を出力するマーカー分析部と、
前記マーカー分析部から出力される制御信号に応じて、前記マーカー解読部から出力されるマーカーを、更新させ、前記暗号化キーを用いてエンクリップションして、前記バッファに出力するマーカー更新及び暗号化部と、
を備えた請求項２４に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項３６】　前記マーカー分析及び処理部は、暗号化キーを貯蔵して前記マーカー解読部とマーカー更新及び暗号化部に出力する暗号化キー貯蔵部をさらに備えた請求項３５に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項３７】　前記マーカー分析部は、前記コピー防止（ＣＰ）情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写

されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写が可能か否かを判別する請求項３５に記載のディジタル磁気記録再生システムの複写防止装置。

【請求項３８】　前記バッファは、
前記マーカー分析及び処理部から出力される更新されエンクリップションされたマーカーを一時貯蔵した後前記マーカー検出及び挿入部に出力するマーカーバッファと、
前記マーカー分析及び処理部から出力されるコントロールワードを一時貯蔵した後前記ディスクランブラに出力するコントロールワードバッファと、
を備えた請求項２０に記載のディジタル磁気記録再生システムの複写防止装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル記録再生システムの複写防止方法及び装置に関する。特に、複写防止機能に対する情報と機能実行のためのマーカー(Marker)を暗号化し挿入して、複写防止機能を行い、プログラム供給者の所望の多様な複写防止機能が実現できるディジタル磁気記録再生システムの複写防止方法及び装置に関する。

【０００２】

【従来の技術】従来の複写防止方法は、米国特許第４、８１９、０９８号に挙げられている。この方法は、ＶＣＲ内の自動利得制御（ＡＧＣ）回路に干渉を起こす信号をビデオ波形に挿入して、テープに記録する方法である。この方法において、上記テープを再生してＴＶを通じて視聴する場合、干渉信号は、ＴＶのＡＧＣ回路に影響を与えず、正常のディスプレイが可能である。

【０００３】しかし、再生された信号を他のＶＣＲが録画する場合、すなわち複写する場合、干渉信号が録画するＶＣＲのＡＧＣ回路に干渉を起こすことにより、不正確な信号レベルを記録させる。したがって、複写されたテープを再生する場合、正常のディスプレイはできない。他の例として、米国特許第４、５７１、６４２号は、再生中ＶＣＲ内のサーボ回路を同期させるに使われるコントロールトラックを用いて、複写防止機能を実現した特許である。この特許の原理は、他のテープで複写する時、コントロールトラックが不正確に記録されるように、ビデオ信号を変化させることである。

【０００４】さらに、他の例として、米国特許第４、５７７、２１６号は、ビデオ信号のクロマバスト部分に、位相ノイズのようなものを挿入して複写防止機能を実現している。

【０００５】

【発明が解決しようとする課題】上記のような方法は、すべてＴＶ回路とこれに対応するＶＣＲの回路との間の感度の差を用いる方法である。従って、このような方法

で複写防止されたテープは、一部のＶＣＲでは複写防止できない場合があり、一部のＴＶでは原本も正常的にディスプレイできない短所がある。

【０００６】また、上記のような方法は、アナログ方式の複写防止方法である。このようなアナログ方式の複写防止方法は、ＮＴＳＣ級映像についてアナログＶＣＲへの複写を防ぐにおいて有用な方法である。しかし、ＡＴＶの高解像度映像の場合は、アナログＶＣＲよりはディジタルＶＣＲを用いた複写がされるので、アナログ方式の複写防止方法を適用し難い問題点がある。

【０００７】従って、本発明の目的は、ディジタルＴＶに適用できる多様な複写防止機能と共に、プログラム供給者が望む複写防止機能を選択できるようにしたディジタル磁気記録再生システムの複写防止方法及び装置を提供することにある。

【０００８】

【課題を解決するための手段】本発明によるディジタル磁気記録再生システムの複写防止方法は、オーディオ及びビデオビットストリームをスクランブリングするためのコントロールワードと不法複写防止のためのコピー防止（ＣＰ）情報とにより作られたマーカーを、暗号化キーを用いてエンクリップションして、前記コントロールワードでスクランブリングされたオーディオ及びビデオビットストリームで、マルチプレキシングして伝送するオーディオ及びビデオ信号伝送工程と、前記伝送されたビットストリームからマーカーを検出し、暗号化されたキーを用いてディクリップション及び分析して、複写を許容するか否かを決定して、検出されたマーカーを更新させビデオテープに記録させ、前記マーカーからコントロールワードを発生してディスクランブリングして、ディスプレイできるようにモニターに出力するオーディオ及びビデオ信号受信及び記録工程と、を備えており、そのことにより上記目的が達成される。

【０００９】ある実施形態では、前記マーカーは、前記ビットストリーム内の伝送プライベートデータフィールドに位置する。

【００１０】ある実施形態では、前記マーカーは、不法複写防止のためのコピー防止（ＣＰ）情報の記録されたコピー防止（ＣＰ）情報領域と、ディスクランブリングのためのコントロールワードが記録されたコントロールワード領域と、を有している。

【００１１】ある実施形態では、前記マーカーは、８バイトよりなる。

【００１２】ある実施形態では、前記コピー防止（ＣＰ）情報領域は、１バイトよりなる。ある実施形態では、前記コントロールワード領域は、４バイトよりなる。

【００１３】ある実施形態では、前記コピー防止（ＣＰ）情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマッティングされる。

【００１４】ある実施形態では、前記世代複写制御フィールドは、プログラムの複写を許す回数を制限するための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドと、を有している。

【００１５】ある実施形態では、前記オーディオ及びビデオ伝送工程は、オーディオ及びビデオビットストリームをエンコーディングするオーディオ及びビデオビットストリームエンコーディング工程（１）と、スクランブリングのためのコントロールワードを発生するコントロールワード発生工程（２）と、前記発生されたコントロールワードを用いて前記エンコーディングされたオーディオ及びビデオビットストリームをスクランブリングするスクランブリング工程（６）と、不法複写防止のためのコピー防止（ＣＰ）情報を発生するコピー防止（ＣＰ）情報発生工程（３）と、前記発生されたコントロールワードと前記コピー防止（ＣＰ）情報を用いてマーカーを発生し暗号化されたキーを用いてエンクリップションするマーカー発生及びエンクリップション工程（４、５）と、前記スクランブリングされたオーディオ及びビデオビットストリームとエンクリップションされたマーカーをマルチプレキシングして伝送するマルチプレキシング及び伝送工程と、を包含している。

【００１６】ある実施形態では、前記オーディオ及びビデオ信号受信工程は、前記伝送されたビットストリームをディマルチプレキシングしてマーカーを検出し、暗号化されたキーを用いてディクリップションするマーカー検出工程（１１、１２）と、前記検出されたマーカーを分析して複写を許容するか否かを決定しコントロールワードを検出するマーカー分析工程（１３）と、前記検出されたコントロールワードで、前記伝送されたオーディオ及びビデオビットストリームをディスクランブリング及びディコーディングして、音声及び映像信号を出力するオーディオ及びビデオディコーディング工程（１４、１５）と、前記マーカー分析結果複写可能な場合、前記検出されたマーカーを、更新させ暗号化されたキーを用いてエンクリップションして挿入するマーカー挿入工程（１６、１７、１８）と、を包含している。

【００１７】ある実施形態では、前記マーカー分析工程（１３）は、前記検出されたマーカーから不法複写防止のためのコピー防止（ＣＰ）情報を検出するコピー防止（ＣＰ）情報検出工程と、前記検出されたコピー防止（ＣＰ）情報内のプログラムの複写を許容する回数を制限するための容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写が可能か否かを判別して処理する複写回数制限工程と、前記検出されたマーカーより、ディスクランブリングのためのコントロールワードを検出するコントロールワード検出工程と、を包含している。

【００１８】ある実施形態では、前記複写回数制限工程は、前記許容世代フィールドの許容世代と、現在世代フィールドの現在世代とを比較して、前記許容世代が現在世代以下かを判断する工程と、前記判断結果前記許容世代が現在世代以下なら複写を不可能にする工程と、前記判断結果前記許容世代が現在世代以下でなければ複写を可能にし、前記マーカー挿入工程に進む工程と、を包含している。

【００１９】ある実施形態では、前記複写を不可能にする工程は、複写後、再生が不可能になるようにコントロールワードを破壊したり、出力できないようにする。

【００２０】ある実施形態では、前記コントロールワードは、周期的に変化される。

【００２１】ある実施形態では、前記コントロールワードは、０．６秒間隔に変わる。

【００２２】ある実施形態では、前記マーカーは、前記コントロールワードが変わる毎に、前記ビットストリーム内のプライベートデータフィールドに位置する。

【００２３】ある実施形態では、前記マーカ挿入工程は、前記マーカー分析結果複写可能な場合は前記マーカーを更新させる工程（１６）と、前記更新されたマーカーを暗号化されたキーを用いてエンクリップションする工程（１７）と、前記エンクリップションされたマーカーを次に現れるマーカーと交替して挿入する工程（１８）と、を包含している。

【００２４】ある実施形態では、前記暗号化されたキーは、別途の伝送路を通じて伝送され貯蔵される。

【００２５】ある実施形態では、前記暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵される。

【００２６】本発明によるディジタル磁気記録再生システムの複写防止装置は、入力されるビットストリームから、マーカーを検出し、更新されたマーカーを、前記ビットストリームに挿入して出力するマーカー検出及び挿入部と、前記マーカー検出及び挿入部から出力されるエンクリップションされたマーカーを、暗号化されたキーを用いてディクリップションし分析して、ビットストリームをディスクランブリングさせるためのコントロールワードを出力し、ディクリップションされたマーカーを、更新させ暗号化されたキーを用いてエンクリップションさせ出力するマーカー分析及び処理部と、前記マーカー分析及び処理部から出力されるコントロールワードと、更新されエンクリップションされたマーカーとをバッファリングして、前記更新されエンクリップションされたマーカーを、前記マーカー検出及び挿入部で挿入できるように出力するバッファと、前記バッファから出力されるコントロールワードを用いて、前記マーカー検出及び挿入部を通じて出力されるビットストリームを、ディスクランブリングするディスクランブラと、備えており、そのことにより上記目的が達成される。ある実施形態では、前記暗号化されたキーは、別途の伝送路を通じて伝送され貯蔵される。

【００２７】ある実施形態では、前記暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵される。

【００２８】ある実施形態では、前記マーカーは、前記ビットストリーム内の伝送プライベートデータフィールドに位置する。

【００２９】ある実施形態では、前記マーカーは、不法複写防止のためのコピー防止（ＣＰ）情報が記録されたコピー防止（ＣＰ）情報領域と、ディスクランブリングのためのコントロールワードの記録されたコントロールワード領域と、を備えている。

【００３０】ある実施形態では、前記マーカーは、８バイトよりなる。

【００３１】ある実施形態では、前記コピー防止（ＣＰ）情報領域は、１バイトよりなる。ある実施形態では、前記コントロールワード領域は、４バイトよりなる。

【００３２】ある実施形態では、前記コピー防止（ＣＰ）情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマッティングされる。

【００３３】ある実施形態では、前記世代複写制御フィールドは、プログラムの複写を許容する回数を制限するための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドと、を備えている。

【００３４】ある実施形態では、前記コントロールワードは、周期的に変わる。

【００３５】ある実施形態では、前記コントロールワードは、０．６秒間隔に変わる。

【００３６】ある実施形態では、前記マーカーは、前記コントロールワードが変わる毎に前記ビットストリーム内のプライベートデータフィールドに位置する。

【００３７】ある実施形態では、前記マーカー検出及び挿入部は、前記更新されたマーカーを次に現れるマーカーと交替して挿入する。

【００３８】ある実施形態では、前記マーカー検出及び挿入部は、入力されるビットストリームからエンクリップトされたマーカーを検出して、前記マーカー分析及び処理部に出力し、前記ビットストリーム内におけるエンクリプトされたマーカーの位置を知らせるマーカー検出フラグ信号を、前記ディスクラブラに出力して、前記ディスクランブラが初期化される基準信号として使われるようにしビットストリームを出力するマーカー検出部と、前記マーカー検出部から出力されるマーカー検出フラグ信号に応じて、前記マーカー検出部から出力されるビットストリームに、前記バッファから出力される更新されエンクリップションされたマーカーを挿入して、前

記ディスクランブラに出力するマーカー挿入部と、を備えている。ある実施形態では、前記マーカー分析及び処理部は、前記マーカー検出及び挿入部から出力されるエンクリップションされたマーカーを、暗号化されたキーを用いてディクリップションするマーカー解読部と、前記マーカー解読部から出力されるマーカー内部のコピー防止（ＣＰ）情報を分析して、複写が許容される場合、前記バッファにコントロールワードを出力しマーカーを更新するための制御信号を出力するマーカー分析部と、前記マーカー分析部から出力される制御信号に応じて、前記マーカー解読部から出力されるマーカーを、更新させ、前記暗号化キーを用いてエンクリップションして、前記バッファに出力するマーカー更新及び暗号化部と、を備えている。

【００３９】ある実施形態では、前記マーカー分析及び処理部は、暗号化キーを貯蔵して前記マーカー解読部とマーカー更新及び暗号化部に出力する暗号化キー貯蔵部をさらに備えている。

【００４０】ある実施形態では、前記マーカー分析部は、前記コピー防止（ＣＰ）情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写が可能か否かを判別する。

【００４１】ある実施形態では、前記バッファは、前記マーカー分析及び処理部から出力される更新されエンクリップションされたマーカーを一時貯蔵した後前記マーカー検出及び挿入部に出力するマーカーバッファと、前記マーカー分析及び処理部から出力されるコントロールワードを一時貯蔵した後前記ディスクランブラに出力するコントロールワードバッファと、を備えている。

【００４２】

【発明の実施の形態】本発明によるディジタル磁気記録再生システムの複写防止方法及び装置は、ＤＶＣＲが色々の信号を全部ビデオテープに録画できることを強調して、入力されうる多種の信号を大きく二種に分類し、各信号別に異なる複写防止機能を実行させる。本発明による上記方法は、まず、地上(Terrestrial) 放送、衛星放送、ケーブルから伝送される信号を放送信号に分類し、この信号を録画する時は次のように三種の複写防止機能を有する。この三種の複写防止機能は、テープへの録画絶対不可機能、テープへの自由な録画及び複写許容機能、及びビデオテープへの１世代録画可能と録画されたテープの複写不可機能に分かれる。

【００４３】ここで、三番目の機能であるビデオテープへの１世代録画可能と録画されたテープの複写不可機能は、ＴＶ受信機から送られる信号をテープで１回録画するのは可能である。１回録画されたテープを再生する場合視聴できるが、他のＤＶＣＲでこの信号を録画することは不可能である。

【００４４】二番目の分類は、レンタルテープであって、記録媒体に記録された信号に分類する。この信号を録画する時の複写防止機能は、前述したテープへの録画絶対不可機能及びテープへの自由な録画及び複写許容機能と類似であり、次のような三種の複写防止機能を有する。この三種の複写防止機能は、他のテープへの複写絶対不可、他のテープへの自由な複写許容、及び他のテープへの１世代複写許容に分かれる。ここで、他のテープへの１世代複写許容機能は、レンタルテープ原本からは複写本が作られるが、複写本からさらに他の複写本を作ることを防ぐ方法であり、ＤＡＴで使われる複写防止機能である。

【００４５】本発明は、上記の機能をプログラム供給者がプログラム供給時に選択できるようにする長所を有する。このため、プログラム供給者は、所望の複写防止機能に対する情報、すなわちマーカーをプログラム内の定められたフィールドに挿入してプログラムを分配する。プログラム供給者が伝送データ上に挿入して伝送するマーカーは、暗号化されている。マーカーを解読できる暗号キーは、不法複写を防ぐために、一定間隔に、例えば一か月に１回ほど、電話線のような別途の伝送路を通じて伝送され、複写防止装置内に貯蔵される。

【００４６】上記の複写防止機能を実現する複写防止装置は、ＡＴＶディコーダとディジタルＶＣＲが一体型のシステムにおいて、ＡＴＶディコーダとディジタルＶＣＲとの間のインタフェース過程で、ディジタル複写防止機能を行わせ、受信された暗号化キーを用いて、受信されたプログラムのマーカーを解読し判断して、それぞれの複写防止機能による他の機能を行う。

【００４７】本発明によるディジタル磁気記録再生システムの複写防止方法は、図１に示したオーディオ及びビデオ信号伝送工程と、図２に示したオーディオ及びビデオ信号受信及び記録工程により行われる。

【００４８】オーディオ及びビデオ信号伝送工程は、オーディオ及びビデオビットストリームをスクランブリングするためのコントロールワードと、不法複写防止のためのコピー防止（ＣＰ）(Copy Protection)情報により、作られたマーカーを、暗号化されたキーを用いてエエンクリップションして、コントロールワードにスクランブリングされたオーディオ及びビデオビットストリームで、マルチプレキシングして伝送することである。プログラム製作者によって、マーカーが作られた状態であり、オーディオ及びビデオビットストリームと共に、マルチプレキシングされ伝送される。

【００４９】すなわち、オーディオ及びビデオ信号伝送工程は、図１に示したように、オーディオ及びビデオビットストリームをエンコーディングするオーディオ及びビデオビットストリームエンコーディング工程（１）、スクランブリングのためのコントロールワードを発生するコントロールワード発生工程（２）、発生されたコン

トロールワードを用いて、前記エンコーディングされたオーディオ及びビデオビットストリームをスクランブリングするスクランブリング工程（６）、不法複写防止のためのコピー防止（ＣＰ）情報を発生するコピー防止（ＣＰ）情報発生工程（３）、発生されたコントロールワードと前記コピー防止（ＣＰ）情報を用いて、マーカーを発生し、暗号化されたキーを用いてエンクリップションするマーカー発生及びエンクリップション工程（４、５）、及び、スクランブリングされたオーディオ及びビデオビットストリームと、エンクリップションされたマーカーをマルチプレキシングして伝送するマルチプレキシング及び伝送工程（７）によって行われる。

【００５０】また、オーディオ及びビデオ信号受信及び記録工程は、伝送されたビットストリームからマーカーを検出して、暗号化されたキーを用いてディクリップション及び分析して、複写を許容するか否かを決定して、検出されたマーカーが更新されビデオテープに記録される。マーカーからコントロールワードが発生してディスクランブリングして、ディスプレイできるように、モニターに出力される。プログラム製作者から伝送されたオーディオ及びビデオ信号は、マーカーによって記録されたり、ディスプレイされる。

【００５１】すなわち、オーディオ及びビデオ信号受信及び記録工程は、図２に示したように、伝送されたビットストリームをディマルチプレキシングして、マーカーを検出し暗号化されたキーを用いてディクリップションするマーカー検出工程（１１、１２）、検出されたマーカーを分析して複写を許容するか否かを決定しコントロールワードを検出するマーカー分析工程（１３）、検出されたコントロールワードに伝送されたオーディオ及びビデオビットストリームを、ディスクランブリング及びディコーディングして、音声及び映像信号を出力するオーディオ及びビデオディコーディング工程（１４、１５）、及びマーカー分析結果複写可能な場合、検出されたマーカーを更新させ、暗号化されたキーを用いてエンクリップションして挿入するマーカー挿入工程（１６、１７、１８）によって行われる。

【００５２】この過程を詳しく説明すれば次の通りである。まず、プログラム製作者は、オーディオ及びビデオビットストリームをエンコーディングし（１）、スクランブリングのためのコントロールワードを発生した後（２）、発生されたコントロールワードを用いてエンコーディングされたオーディオ及びビデオビットストリームをスクランブリングする（６）。

【００５３】次に、不法複写防止のためのコピー防止（ＣＰ）情報を発生し（３）、発生されたコントロールワードとコピー防止（ＣＰ）情報を用いてマーカーを発生し（４）、暗号化されたキーを用いてエンクリップションする（５）。

【００５４】最後に、スクランブリングされたオーディオ及びビデオビットストリームとインクリップションされたマーカーを、マルチプレキシングして（７）プログラム記録または再生のために伝送する。

【００５５】伝送されたビットストリームをディマルチプレキシングしてマーカーを検出し、（１１）、暗号化されたキーを用いて、ディクリップションして、ディクリップションされたマーカーを出力する（１２）。検出されディクリップションされたマーカーを分析して複写を許容するか否かを決定しコントロールワードを検出する（１３）。

【００５６】検出されたコントロールワードに伝送されたオーディオ及びビデオビットストリームを、ディスクランブリング及びディコーディングして、音声及び映像信号をモニターに出力してディスプレイできるようにする（１４、１５）。

【００５７】また、マーカー分析結果複写可能な場合、検出されたマーカーを更新させ、暗号化されたキーを用いてエンクリップションして、オーディオ及びビデオビットストリームに挿入して記録する（１６、１７、１８）。

【００５８】ここで、図３に基づいて、マーカーが挿入される位置を見る。伝送されるビットストリームは、固定長、すなわち１８８バイトからなる伝送パケットより構成される。そのうち、ビットストリームの前端に伝送ヘッダが位置する。伝送ヘッダは、再び４バイトの固定長フィールドと可変長のアダップテーションフィールド(adaptation field)に分かれる。そして、アダップテーションフィールド内の１フィールドであって、伝送プライベートデータフィールドが存在する。伝送プライベートデータフィールドは、再びＩＤフィールドとエンクリップションされた状態のマーカーより構成される。ＩＤフィールドは、伝送プライベートデータフィールドが本発明の複写防止方法のために用いられるフィールドであることを知らせるための識別子の機能を有し、ＩＤフィールド以後に存在するエンクリップションされたマーカーにより本発明の複写防止機能を実現する。

【００５９】マーカーが暗号化されたキーを用いてディクリップションされれば、マーカーは、不法複写防止のためのコピー防止（ＣＰ）情報が記録されたコピー防止（ＣＰ）情報領域と、ディスクランブリングのためのコントロールワードＣＷが記録されたコントロールワード領域と、リザーブド(Reserved)領域に分かれる。すなわち、ディクリップションされたマーカーは８バイトよりなり、１バイトよりなるコピー防止（ＣＰ）情報領域と３バイトよりなるリザーブド領域と４バイトよりなるコントロールワード領域に分かれる。

【００６０】ここで、コピー防止（ＣＰ）情報はプログラムの複写可能回数を制限する世代複写制御フィールドを含めてフォーマッティングされるが、世代複写制御フィールドはプログラムの複写を許容する回数を制限する

ための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドよりなる。

【００６１】次に、オーディオ及びビデオ信号受信及び記録工程のマーカー分析工程（１３）を詳しく説明する。マーカー分析工程（１３）は検出されたマーカーから不法複写防止のためのＣＰ情報を検出するコピー防止（ＣＰ）情報検出工程、検出されたコピー防止（ＣＰ）情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写できるか否かを判別して処理する複写回数制限工程、及び検出されたマーカーからディスクランブリングのためのコントロールワードを検出するコントロールワード検出工程により行われる。すなわち、検出されたマーカーから不法複写防止のためのコピー防止（ＣＰ）情報を検出し、検出されたコピー防止（ＣＰ）情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写可能か否かを判別する。複写の可能な場合、記録させ、複写が不可能な場合は、記録しても再生を不可能にさせる。

【００６２】次いで、検出されたマーカーからディスクランブリングのためのコントロールワードを検出する。ここで、複写回数制限工程は許容世代フィールドの許容世代と、現在世代フィールドの現在世代とを比較して、許容世代が現在世代以下かを判断する工程と、及び判断結果として、許容世代が現在世代以下なら複写が不可能にする工程と、及び判断結果として、許容世代が現在世代以下でなければ複写可能にし、マーカー挿入工程に進む工程により行われる。

【００６３】上記の複写回数制限工程を説明すれば次の通りである。

【００６４】プログラム製作者が設定した許容世代フィールドの許容世代と、現在の複写回数を示す現在世代フィールドの現在世代とを比較して、許容世代が現在世代以下なら、プログラム製作者が設定した複写回数を超えたので複写をこれ以上不可能にする。この際、複写を不可能にする方法は、複写後再生を不可能にコントロールワードを破壊したり、出力できないようにすることである。なぜなら、オーディオ及びビデオビットストリームは、スクランブリングされた状態で記録されるので、コントロールワードがなければ、スクランブリングされたオーディオ及びビデオビットストリームをディスクランブリングできないからである。

【００６５】従って、コントロールワードを破壊すれば、オーディオ及びビデオビットストリームが記録されても再生してデイスプレイできないので、記録が不可能なことと同様になる。この際、コントロールワードは周期的に、すなわち０．６秒間隔に変わるので、次に現れるコントロールワードを全部破壊することにより複写されても再生を不可能にする。また、ビデオテープ内のコントロールトラックを破壊して複写を不可能にすることもできる。

【００６６】一方、マーカーは、コントロールワードが変わる毎にビットストリーム内のプライベートデータフィールドに位置することになる。ここで、コントロールワードは周期的に変わるのでコントロールワードが変わって入力される毎にコントロールワードが含まれたマーカーが入力される。

【００６７】一方、マーカー挿入工程は、マーカー分析結果複写可能な場合はマーカーを更新させる工程（１６）、更新されたマーカーを暗号化されたキーを用いてエンクリップションする工程（１７）、及びエンクリップションされたマーカーを次に現れるマーカーと交替して挿入する工程（１８）により行われる。すなわち、マーカー分析結果複写可能な場合は現在世代フィールドの現在世代を”１”増加させ更新させることによりマーカーを更新させる（１６）。すなわち、現在世代が”１”増加され更新された現在世代フィールドを含むＣＰ情報はコントロールワードと合わせて更新されたマーカーとなる。

【００６８】更新されたマーカーは、再び暗号化されたキーを用いてエンクリップションされ（１７）、次に現れるマーカーと交替され挿入される。すなわち、マーカーは、コントロールワードが変わる毎に入力されるので、コントロールワードが変わる毎に挿入される。言い換えれば、図３に示したようにエンクリップションされたマーカーを検出することと、更新されたマーカーを交替するのは、時間的に共になされるべきである。

【００６９】一方、マーカーをエンクリップション及びディクリップションさせるための暗号化されたキーは、一定間隔に別途の伝送路を通じて伝送され貯蔵された後使われることにより不法複写を完璧に防止しうる。すなわち、マーカーは、暗号化されたキーでエンクリップションされた状態でビットストリームと共に伝送され記録される。スクランブリングされたオーディオ及びビデオビットストリームをディスクランブリングするためのコントロールワードが、マーカーに含まれているので、コントロールワードを得るためには、まずマーカーをディクリップションすべきである。ところが、マーカーをディクリップションするための暗号化キーが周期的に変化されるので、暗号化キーなしでマーカーをディクリップションするのは不可能である。このことによって、不法的にコントロールワードを得ることはさらに難しい。

【００７０】本発明によるディジタル磁気記録再生システムの複写防止装置は、図４に示すように、マーカー検出及び挿入部２１、ディスクランブラ２４、マーカー分析及び処理部２２、及びバッファ２３より構成される。

【００７１】マーカー検出及び挿入部２１は、入力され

るビットストリームからマーカーを検出し、バッファ２３から出力される更新されたマーカーを、すなわち更新されエンクリップションされたマーカーを、入力されるビットストリームに挿入して出力する。

【００７２】マーカー分析及び処理部２２は、暗号化されたキーを用いてマーカー検出及び挿入部２１から出力されるエンクリップションされたマーカーを、ディクリップションし、分析する。このことによって、ビットストリームをディスクランブリングさせるためのコントロールワードを出力する。それから、ディクリップションされたマーカーは、更新され、再び暗号化されたキーを用いてエンクリップションされ出力される。

【００７３】バッファ２３は、マーカー分析及び処理部２２から出力されるコントロールワードＣＷと、更新されエンクリップションされたマーカーＩＥＭとをバッファリングする。更新されエンクリップションされたマーカーＩＥＭは、マーカ検出及び挿入部２１で挿入できるように出力される。

【００７４】ディスクランブラ２４は、バッファ２３から出力されるコントロールワードを用いて、マーカー検出及び挿入部２１を通じて出力されるビットストリームを、ディスクランブリングしてディスプレイできるようにモニターに出力したり、マーカーが挿入されたビットストリームを記録できるようにＤＶＣＲに出力する。ここで、暗号化されたキーは、本発明によるディジタル記録再生システムの複写防止方法のように、一定間隔に別途の伝送路を通じて伝送され貯蔵され著作権の保護効果を倍加させる。

【００７５】このように構成されたディジタル磁気記録再生システムの複写防止装置の動作を説明する前に、図３に基づき伝送ビットストリーム及びマーカーの構造について説明する。

【００７６】ディジタル磁気記録再生システムの複写防止装置において、ディジタル磁気記録再生システムの複写防止方法と同様に、図３に示したように、マーカーは、ビットストリーム内の伝送プライベートデータフィールド(Transfer-private-data-field) に位置している。なお、ディジタル磁気記録再生システムの複写防止装置は、不法複写防止のためのＣＰ情報の記録されたＣＰ情報領域と、ディスクランブリングのためのコントロールワードＣＷが記録されたコントロールワード領域とを含んでいる。

【００７７】ここで、ＣＰ情報は、プログラムの複写可能回数を制限する世代複写制御フィールドを含むフォーマッティングされる。世代複写制御フィールドは、プログラムの複写を許容する回数を制限するための許容世代フィールドと、複写されたプログラムの現在の世代を示す現在世代フィールドよりなる。また、マーカーは８バイトよりなり、このうちＣＰ情報領域は１バイトよりなり、コントロールワード領域は４バイトよりなる。

【００７８】次いで、本発明によるディジタル磁気記録再生システムの複写防止装置の概略的な動作を図４に基づいて説明する。

【００７９】まず、入力されるビットストリームをモニターにディスプレイする過程を説明する。入力されるビットストリームは、マーカー検出及び挿入部２１でマーカーが検出されエンクリップションされた状態で、マーカー分析及び処理部２２に入力される。エンクリップションされたマーカーＥＭは、マーカー分析及び処理部２２で暗号化されたキーを用いてディクリップションされてから分析される。この際、分析されたマーカーからコントロールワードが検出されビットストリームをディスクランブリングさせるために、バッファ２３をバッファリングされた後ディスクランブラ２４に入力される。

【００８０】マーカー検出及び挿入部２１から、マーカーが検出された後のビットストリームは、ディスクランブラ２４でバッファ２３から出力されるコントロールワードによりディスクランブリングされた後、ディスプレイできるようにモニターに出力される。

【００８１】次いで、入力されるビットストリームをＤＶＣＲを通じて記録する過程を説明する。入力されるビットストリームからマーカーを検出し分析する過程は、同一である。すなわち、入力されるビットストリームは、マーカー検出及び挿入部２１でマーカーが検出されエンクリップションされた状態で、マーカー分析及び処理部２２に入力される。

【００８２】コントロールワードを検出するため、エンクリップションされたマーカーＥＭは、マーカー分析及び処理部２２で暗号化されたキーを用いてディクリップションされた後分析される。この際、分析結果によって、記録できるようになったり、不可能になる。記録が不可能な場合は、検出されたコントロールワードを破壊して、記録されても再生が不可能になる。記録が可能な場合は、マーカー内の現在世代フィールドの現在世代を”１”増加させ更新させた後、暗号化されたキーを用いてエンクリップションさせバッファ２３に出力する。更新されエンクリップションされたマーカーは、バッファ２３でバッファリングされた後、マーカー検出及び挿入部２１に出力され入力されるビットストリームに挿入される。

【００８３】一方、コントロールワードは、周期的に、すなわち０．６秒間隔に変化する。マーカーは、コントロールワードが変わる毎にビットストリーム内の伝送プライベートデータフィールドに位置することになる。よって、更新されエンクリップションされたマーカーは、次に現れるマーカーと交替して挿入される。更新されエンクリップションされたマーカーが挿入されたビットストリームは、ディスクランブラ２４をそのまま通過してＤＶＣＲで記録できるように出力される。

【００８４】このように構成されるディジタル磁気記録

再生システムの複写防止装置の細部構成及び動作を添付した図面に基づいて説明する。図５は、図４の細部構成を示した細部構成図である。各部の細部構成を図５に基づいて説明する。

【００８５】マーカー検出及び挿入部２１は、入力されるビットストリームからエンクリプトされたマーカーを検出して、マーカー分析及び処理部２２に出力する。ビットストリーム内におけるエンクリプトされたマーカーの位置を知らせるマーカー検出フラグ信号は、ディスクランブラ２４に出力されて、ディスクランブラ２４が初期化される基準信号として使うようにする。ビットストリームを出力するマーカー検出部３１、及びマーカー検出部３１から出力されるマーカー検出フラグ信号に応じて、マーカー検出部３１から出力されるビットストリームに、バッファ２３から出力される更新されエンクリップションされたマーカーを挿入してディスクランブラ２４に出力するマーカー挿入部３２より構成される。

【００８６】マーカー分析及び処理部２２は、マーカー検出及び挿入部２１のマーカー検出部３１から出力されるエンクリップションされたマーカーを暗号化されたキーを用いてディクリップションするマーカー解読部３３と、マーカー解読部３３から出力されるマーカー内部のＣＰ情報を分析して、複写が許容される場合、バッファ２３にコントロールワードを出力しマーカーを更新するための制御信号を出力するマーカー分析部３４と、及びマーカー分析部３４から出力される制御信号に応じて、マーカー解読部３４から出力されるマーカーを更新させ暗号化されたキーを用いてエンクリップションしてバッファ２３に出力するマーカー更新及び暗号化部３５と、より構成される。ここで、マーカー分析及び処理部２２は、暗号化されたキーを貯蔵して、マーカー解読部３３とマーカー更新及び暗号化部３５に出力する暗号化キー貯蔵部をさらに含めて構成される。

【００８７】また、マーカー分析部３４は、ＣＰ情報内のプログラムの複写を許容する回数を制限するための許容世代フィールドの許容世代と、複写されたプログラムの現在の世代を示す現在世代フィールドの現在世代とを比較して、複写の可能か否かを判別する。

【００８８】バッファ２３は、マーカー分析及び処理部２２から出力される更新されエンクリップションされたマーカーを一時貯蔵した後、マーカー検出及び挿入部２１に出力するマーカーバッファ３６、及びマーカー分析及び処理部２２から出力されるコントロールワードを一時貯蔵してから、ディスクランブラ２４に出力するコントロールワードバッファ３７より構成される。

【００８９】このように構成される本発明によるディジタル磁気記録システムの複写防止装置の動作を図６に基づいて説明する。図６(a)は、伝送されたビットストリームのタイミング図である。図６(b)は、マーカー検出フラグ（ｍ－ｄｅｔ－ｆｌａｇ）のタイミング図である。図６(c)は、マーカー分析部３４から出力されるコントロールワードＣＷ（ｉ）のタイミング図である。図６(d)は、マーカー更新及び暗号化部３５から出力される更新されエンクリップションされたマーカーＩＥＭ（ｉ）のタイミング図である。図６(e)は、マーカーバッファ３６から出力される更新されエンクリップションされたマーカーＩＥＭ（ｉ）のタイミング図である。図６(f)は、コントロールワードバッファ３７から出力されるコントロールワードＣＷ（ｉ）のタイミング図である。伝送されたビットストリーム中には、エンクリップションされたマーカーＥＭ（ｉ）が含まれる。

【００９０】エンクリップションされたマーカーＥＭ（ｉ）を含む伝送されたビットストリームは、図６(a)に示したようになされ、マーカー検出部３１に入力され、エンクリップションされたマーカーＥＭ（ｉ）が検出されマーカー解読部３３に出力される。また、マーカー検出部３１では、エンクリプトされたマーカーの位置を知らせるマーカー検出フラグ信号（ｍ－ｄｅｔ－ｆｌａｇ）を、図６(b)に示したようにエンクリップションされたマーカＥＭ（ｉ）部分に発生させ、エンクリップションされたマーカーＥＭ（ｉ）の含まれたビットストリームと共に、マーカー挿入部３２に出力し、マーカー検出フラグ（ｍ－ｄｅｔ－ｆｌａｇ）をディスクランブラ２４に出力して、コントロールワードバッファ３７から伝送されるコントロールワードＣＷ（ｉ－１）にディスクランブラ２４を初期化させる基準信号として使うようにする。エンクリップションされたマーカーＥＭ（ｉ）は、マーカー解読部３３で暗号化キーによりディクリップションされ、ディクリップションされたマーカーＭ（ｉ）に出力される。ディクリップションされたマーカーＭ（ｉ）はマーカー分析部３４で分析され複写可能か否かを判別する。すなわち、マーカー分析部３４ではディクリップションされたマーカーＭ（ｉ）内のＣＰ情報、すなわち、許容世代フィールドと現在世代フィールドとを比較して、許容世代フィールドが現在世代フィールド以下でなければ、複写可能であると判断する。

【００９１】このように複写が許容される場合、マーカー分析部３４では、図６(c)に示したように、マーカーＭ（ｉ）の一部データであるコントロールワードＣＷ（ｉ）をやや遅延させ、コントロールワードバッファ３７に出力する。この際、マーカー分析部３４では、マーカー更新及び暗号化部３５に制御信号を出力して、マーカーを更新させることを制御させる。すなわち、マーカー解読部３３では、エンクリップションされたマーカーＥＭ（ｉ）から解読に必要な時間遅延以後、ディクリップションされたマーカーＭ（ｉ）を作り、マーカー分析部３４でディクリップションされたマーカＭ（ｉ）から、コントロールワードＣＷ（ｉ）を発生させる。

【００９２】この際、コントロールワードＣＷ（ｉ）は、コントロールワードバッファ３７に伝送され、ディ

スクランブラ２４で使われるまで貯蔵される。マーカー解読部３３から出力されるディクリップションされたマーカーM（ｉ）は、マーカー更新及び暗号化部３５でマーカー分析部３４から出力される制御信号に応じて更新される。すなわち、更新されるデータは、マーカー内の現在世代フィールドに記録されるデータに、以前に記録された現在世代に”１”を加算してなされる。

【００９３】このように更新されたマーカーは、再び暗号化キーによりエンクリップション、すなわち暗号化され図６(c)に示したように、マーカー分析部３４から出力されるコントロールワードCW（ｉ）についてやや遅延された状態で、図６(d)に示したようにマーカーバッファ３６に出力される。すなわち、マーカー解読部３３から出力されるエンクリップションされたマーカーM（ｉ）は、マーカー更新及び暗号化部３５に送られ、暗号化に必要な時間遅延以後に更新されエンクリップションされたマーカＩＥＭ（ｉ）に発生されたマーカーバッファ３６に伝送される。

【００９４】この際、マーカー更新及び暗号化部３５と、マーカー分析部３４から出力される更新されエンクリップションされたマーカーＩＥＭ（ｉ）と、コントロールワードCW（ｉ）が発生する時点と、マーカー挿入部３２とディスクランブラ２４で更新されエンクリップションされたマーカーＩＥＭ（ｉ）とコントロールワードCW（ｉ）を用いる時点、すなわち交替挿入及びディスクランブラ２４の初期化過程での時点が不一致するので、この間マーカーバッファ３６とコントロールワードマーカーバッファ３７でマーカー更新及び暗号化部３５とマーカー分析部３４から出力される更新されエンクリップションされたマーカーＩＥＭ（ｉ）とコントロールワードCW（ｉ）を一時貯蔵する。

【００９５】図６(e)に示したように、マーカーバッファ３６で一時貯蔵され同期を合わせて出力される更新されエンクリップションされたマーカーＩＥＭ（ｉ）は、マーカー挿入部３２でマーカー検出部３１から出力されるビットストリームに挿入される。すなわち、マーカー挿入部３２では、エンクリップションされたマーカーＥＭ（ｉ）が含まれたビットストリームとマーカー検出フラグ信号（ｍ－ｄｅｔ－ｆｌａｇ）をマーカー検出部３１から受信し、エンクリップションされたマーカーＥＭ（ｉ）の位置に交替挿入する更新されエンクリップションされたマーカーＩＥＭ（ｉ）をマーカーバッファ３６から受信し、図６(e)に示したように、エンクリップションされたマーカーＥＭ（ｉ）を含む伝送されたビットストリーム中のマーカー検出フラグ信号（ｍ－ｄｅｔ－ｆｌａｇ）の位置に更新されエンクリップションされたマーカーＩＥＭ（ｉ）を交替挿入する。

【００９６】言い換えれば、マーカー挿入部３２は、マーカー検出フラグ信号（ｍ－ｄｅｔ－ｆｌａｇ）が発生した位置でエンクリップションされたマーカーＥＭ（ｉ＋１）をマーカーバッファ３７から出力される更新されエンクリップションされたマーカＩＥＭ（ｉ）に交替挿入される。

【００９７】ここで、交替挿入する更新されエンクリップションされたマーカーＩＥＭ（ｉ）は、直前に検出されたエンクリップションされたマーカーから作られたものである。従って、図６(e)に示したように、マーカーバッファ３７で一定期間の間貯蔵されてからマーカー挿入部３２に出力される。

【００９８】図６(f)に示したように、コントロールワードバッファ３７で一時貯蔵され同期を合わせて出力されるコントロールワードCW（ｉ－１）は、ディスクランブラ２４でマーカー挿入部３２から出力される伝送されたビットストリームをディスクランブリングするに用いられる。

【００９９】この際、ディスクランブラ２４は、マーカー検出部３１から出力されるマーカー検出フラグ信号（ｍ－ｄｅｔ－ｆｌａｇ）をコントロールワードバッファ３７から出力されるコントロールワードCW（ｉ－１）に初期化させる基準信号とする。すなわち、ディスクランブラ２４では、エンクリップションされたマーカーEM（ｉ）が発生された位置、すなわちマーカー検出フラグ信号（ｍ－ｄｅｔ－ｆｌａｇ）が検出された位置から伝送パケットのペイロード(payload)が始まる前の期間の間、コントロールワードバッファ３７から出力されるコントロールワードCW（ｉ－N）に初期化されるべきである。ここで、Nは任意の”０”より大きい自然数であって、コントロールワードCW（ｉ－N）は、エンクリップションされたマーカEM（ｉ）よりN個以前に伝送されたエンクリップションされたマーカーEM（ｉ－N）から作られたコントロールワードである。この”N”はディスクランブラ２４の初期化時点を任意に制御できるようにする。

【０１００】

【発明の効果】以上述べたように、本発明は、プログラム供給者が複写防止機能を選択でき、ＧＡフォーマット内に限られたフィールドを用いるので、複写防止機能のための別途のフォーマット変換装置が不要であり、記録するデータ量の増加もないので既存のディジタルＶＣＲを変換させず複写防止機能を行える。

【図面の簡単な説明】

【図１】本発明による複写防止方法のオーディオ及びビデオ信号伝送工程を示す流れ図である。

【図２】本発明による複写防止方法のオーディオ及びビデオ信号受信及び記録工程を示す流れ図である。

【図３】本発明による伝送ストリームの構造図である。

【図４】本発明による複写防止装置の概略的な構成を示すブロック図である。

【図５】図４の細部構成を示すブロック図である。

【図６】(a)～(f)は、図５の各部の信号波形図である。

23

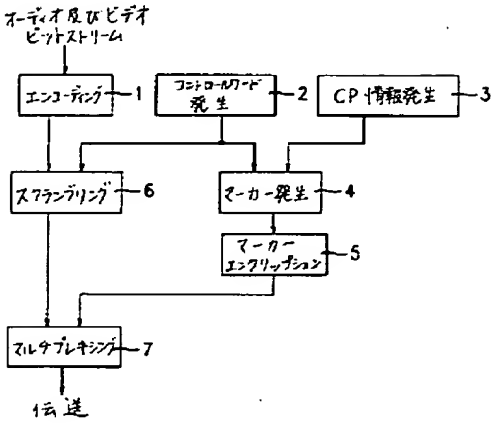
【符号の説明】

２１　マーカー検出及び挿入部
２２　マーカー分析及び処理部
２３　バッファ部
２４　ディスクランブラ
３１　マーカー検出部

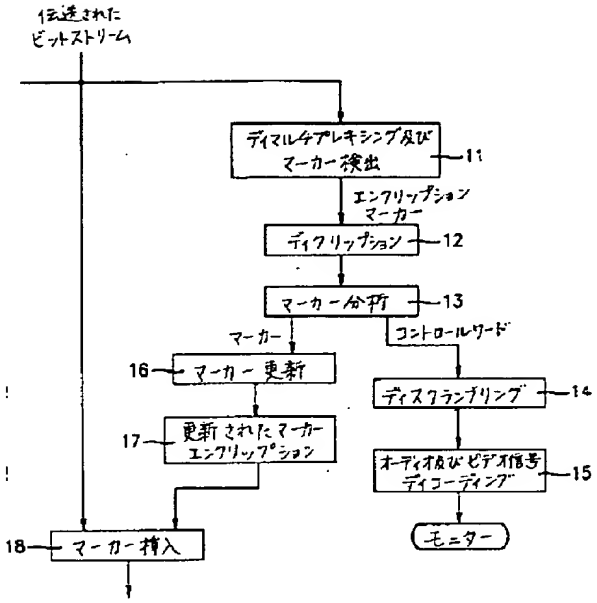
24

３２　マーカー挿入部
３３　マーカー解読部
３４　マーカー分析部
３５　マーカー更新及び暗号化部
３６　マーカーバッファ
３７　コントロールワードバッファ

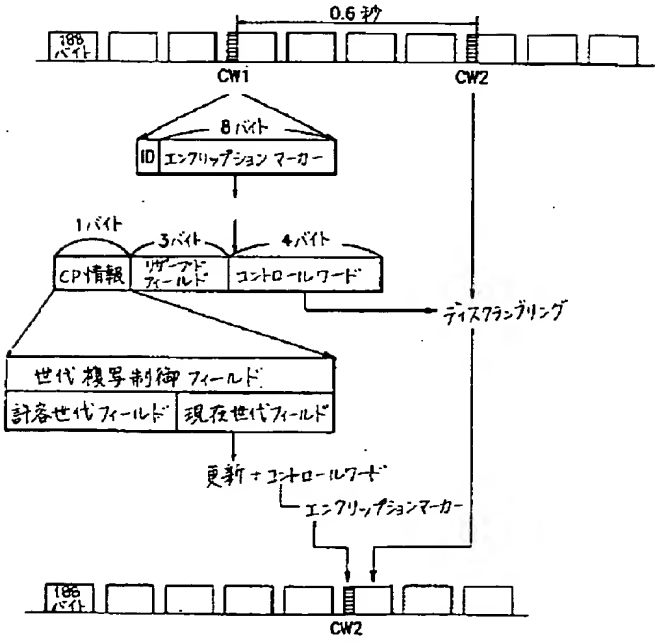
【図１】



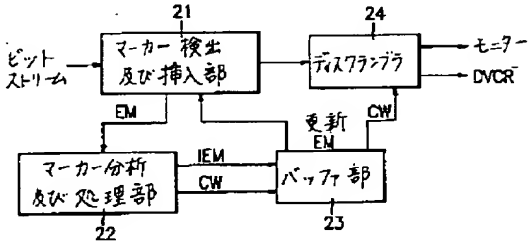
【図２】



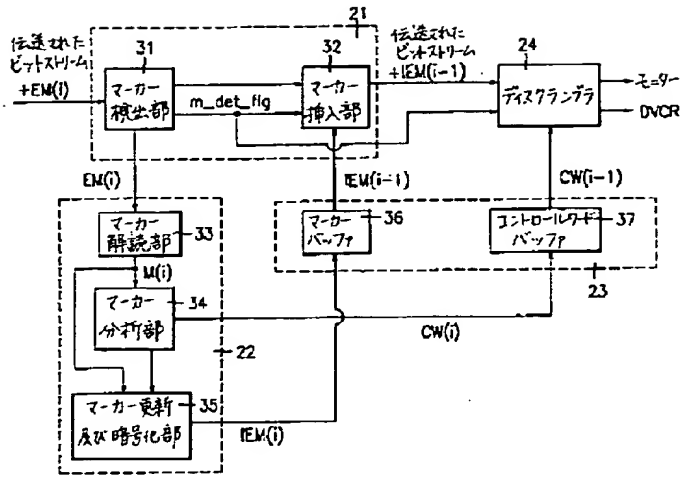
【図３】



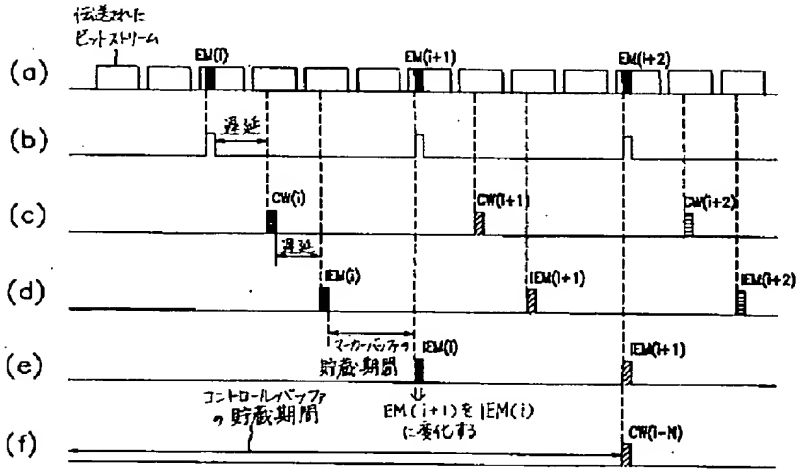
【図４】



【図５】


伝送されたビットストリーム +EM(i)
21
31
32
24
マーカー検出部
m_det_flg
マーカー挿入部
伝送されたビットストリーム +IEM(i-1)
ディスクランブラ
モニター
DVCR
EM(i)
IEM(i-1)
CW(i-1)
マーカー解読部 33
マーカーバッファ 36
コントロールワードバッファ 37
23
M(i)
マーカー分析部 34
22
CW(i)
マーカー更新及び暗号化部 35
IEM(i)

【図６】


伝送されたビットストリーム
(a)
EM(i)
EM(i+1)
EM(i+2)
(b)
遅延
(c)
CW(i)
CW(i+1)
CW(i+2)
遅延
(d)
IEM(i)
IEM(i+1)
IEM(i+2)
マーカーバッファ
(e)
貯蔵期間
IEM(i)
IEM(i+1)
コントロールバッファの貯蔵期間
EM(i+1)をIEM(i)に変化する
(f)
CW(i-N)

DIALOG(R)File 352:DERWENT WPI
(c)1999 Derwent Info Ltd. All rts. reserv.

010773360 **Image available**
WPI Acc No: 96-270313/199628
Copy prevention method for digital magnetic recording apparatus, esp. HDTV VCR - encrypting marker formed by control word for scrambling audio and video bit straps, using encoding key to prevent illegal copying, multiplexing marker with straps,and detecting marker after transmission
Patent Assignee: LG ELECTRONICS INC (GLDS); KINSEISHA KK (GLDS)
Inventor: PARK T J
Number of Countries: 006 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 716544	A2	19960612	EP 95308674	A	19951201	H04N-005/913	199628 B
JP 8237596	A	19960913	JP 95318398	A	19951206	H04N-005/91	199647
EP 716544	A3	19970618	EP 95308674	A	19951201	H04N-005/913	199737
US 5689559	A	19971118	US 95566000	A	19951201	H04N-007/16	199801
CN 1131796	A	19960925	CN 95121501	A	19951208	G11B-020/10	199801

Priority Applications (No Type Date): KR 9433336 A 19941208
Cited Patents: No-SR.Pub; EP 267039; EP 498617; EP 580367; EP 581227; EP 589459
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
EP 716544	A2	E	16			
Designated States (Regional): DE FR GB						
JP 8237596	A		14			
US 5689559	A		14			

Abstract (Basic): EP 716544 A

The copy prevention method includes an audio and video signal transmitting process which involves encrypting a marker formed (4) by a control word (2) for scrambling (6) audio and video bit straps. An encoding key prevents illegal copying. The marker is multiplexed with the audio and video bit strips scrambled by the control word.

An audio and video signal receiving and recording process detects the marker from the transmitting bit strips, decrypts and analyses it using an encoded key to determined whether copying is permitted or not. The marker is updated and recorded on the video tape. The control word is generated from the marker to perform descrambling and supply the audio and video signals to a monitor for display.

ADVANTAGE - Allows program supplier to select one of several copy prevention functions as required.

Dwg.1/6

Abstract (Equivalent): US 5689559 A

The copy prevention method includes an audio and video signal transmitting process which involves encrypting a marker formed (4) by a control word (2) for scrambling (6) audio and video bit straps. An encoding key prevents illegal copying. The marker is multiplexed with the audio and video bit strips scrambled by the control word.

An audio and video signal receiving and recording process detects the marker from the transmitting bit strips, decrypts and analyses it using an encoded key to determined whether copying is permitted or not. The marker is updated and recorded on the video tape. The control word

is generated from the marker to perform descrambling and supply the audio and video signals to a monitor for display.

ADVANTAGE - Allows program supplier to select one of several copy prevention functions as required.

Dwg.1/6

Derwent Class: W04

International Patent Class (Main): G11B-020/10; H04N-005/91; H04N-005/913; H04N-007/16

International Patent Class (Additional): H04N-005/92; H04N-007/167